IPSec THROUGH L2TP

TECHNICAL FIELD

[0001] This invention provides a technique for enabling secure Internet communication between two entities.

BACKGROUND ART

[002] IPsec (Internet Security Protocol) is a protocol promulgated by the Internet Engineering Taskforce (ITEF) for establishing security at the network (packet) processing layer. Currently, the IPsec protocol shows promise for Virtual Private Network and remote dial-up applications. However, a user that employs the IPsec protocol usually incur difficulties in traversing Network Address Translation (NAT) devices and firewalls over which the user has no control. Such difficulties greatly diminish the value of using the IPsec protocol. For that reason, most vendors of IPsec security hardware/software have developed proprietary tunneling protocols to transport IPsec packets in an effort to overcome this problem.

[003] The use of a proprietary tunneling protocol incurs certain disadvantages as compared to use of an open (non-proprietary) tunneling protocol. Unlike an open tunneling protocol whose specification is widely disseminated, the details associated with proprietary tunneling protocols usually remain confidential, affording less confidence in the protocols' security properties. Thus, with most proprietary tunneling protocols, the associated source code has not enjoyed peer review and the attendant identification of faults capable of exploitation by hackers. Moreover, opening tunneling protocols generally have no license restrictions in contrast to proprietary tunneling protocols.

[004] Thus, there is a need for an open tunneling protocol for transporting IPsec packets that overcomes the disadvantages of the prior art.

BRIEF SUMMARY OF THE INVENTION

[005] Briefly, in accordance with a first preferred embodiment of the invention, there is provided a technique for sending an IPsec packet from a first IPsec client to a second IPSec client such that the packet remains unaffected in the event traversal through a firewall and/or a Network Address Translation (NAT) device. To accomplish such IPsec packet transmission, the IPsec packet is wrapped in open (e.g., non-proprietary) tunneling protocol format, such as the Layer-2 Tunneling Protocol (L2TP) format, and is received at a L2TP network server within a communications network from the first IPsec client. The L2TP network server sets up a L2TP tunnel to the second IPsec client and then establishes a security association between the IPsec clients. Thereafter, the L2TP network server transmits the packet to the second IPsec client such that packet remains unaffected in the event traversal through a firewall and/or Network Address Translation device.

[006] The L2TP may receive L2TP-formatted packets from the first IPsec client via dedicated connection (e.g., a tunnel) opened by the first IPsec client. Alternatively, the first IPsec client may access the L2TP network server through the public Internet, provided that the L2TP network server firewall rules allow publicly routed traffic. If one or more NAT devices separate the first and second IPsec clients, both clients may commence a communications session by each opening a tunnel to the L2TP network server, thus allowing the clients to communicate with each other while bypassing any NAT device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] FIGURE 1 illustrates a first embodiment of a network architecture for enabling a first IPsec client to communicate an IPsec-formatted packet to a second IPsec client;

[0008] FIGURE 2 illustrates a second embodiment of a network architecture for enabling a first IPsec client to communicate an IPsec-formatted packet to a second client; and

[0009] FIGURE 3 illustrates an embodiment of a network architecture for enabling a first IPsec client to communicate an IPsec-formatted packet to a second client.

DETAILED DESCRIPTION

[0010] FIGURE 1 depicts a first network architecture 10 for enabling a first IPsec client, represented by IPsec gateway 12, to reliably send one or more IPsec-formatted packets to a second IPsec client 14 (e.g., a IPsec security device associated with a personal computer 15) without any deleterious effects associated with traversing any Network Address Translation device(s) and/or firewalls. The network 10 includes an open (non-proprietary) format tunneling protocol network server, such as a Layer 2 Tunneling Protocol (L2TP) network server 16. In the illustrated embodiment of FIG. 1, the L2TP network server 16 is coupled directly to the IPsec gateway 12 via a common Local Area Network (LAN), depicted as an Ethernet LAN 18. In this way, the L2TP network server 16 can communicate directly with the IP gateway 12 without traversing any firewalls, such as firewall 20 that protects the network 18.

[0011] The L2TP network server 16 functions to create individual L2TP tunnels within the network 10 to different end points such that the L2TP-formatted packets carried by the tunnel unaffected upon passage through any Network Address Translation (NAT) devices and/or firewalls. Thus, for example, the L2TP network server 16 can create a tunnel 21 to an Internet Service Provider network 26 serving the IPsec client 14 so that p L2TP-formatted packets carried by the tunnel remain unaffected by the NAT device 22.

[0012] To send a packet to the IPsec client 14 via the L2TP network server 16, the first IPsec client (i.e., the IPsec gateway 12 of FIG. 1) obtains a private realm address for the IPsec client 14 from the ISP network 26. The private realm address is typically subject to address translation by the NAT 22 and scrutiny by the ISP's firewall (not shown). Thus, were the IPsec gateway 12 to send an IPsec-formatted packet to the private realm address by routing the packet through the router 25, the Public Internet 24, the NAT 22 and the IPS network 26, transmission difficulties would likely result.

[0013] To avoid such difficulties, data transmission in accordance with the invention commences with the IPsec gateway 12 opening an L2TP tunnel 28 with the L2TP network server 16. After opening the tunnel, the IPsec gateway 12 obtains an address associated with the end of the tunnel 28 at the L2TP network server 16. With a tunnel now open to the L2TP network server 16, the IPsec gateway 12 wraps each IPsec packet in a L2TP format, typically by encapsulating the IPsec packet in an L2TP shell for transmission to the L2TP network server using the address associated with the end of the tunnel 28 that terminates with the server.

[0014] Upon receipt of the L2TP-formatted embodying the IPsec packet, the L2TP network server 16 then allows the IPsec gateway 12 (the first IPsec client) to establish a security associated with the IPsec client 14 through the tunnel 21. Once the security association is made, the L2TP network server 16 sends each L2TP-wrapped IPsec packet received from the IPsec gateway 12 via the tunnel 21 to the IPsec client 14,

[0015] To facilitate packet transmission in the manner described, the L2TP network server 16 can distribute to the IPsec gateway 12 virtually any address that is designated for the end of the tunnel 28 provided such address doesn't conflict with the private realm address for the ISP network 26. For that reason, the L2TP network server 16 should preferably distribute separate private realm addresses to avoid reserving a large range of potential addresses associated with the end of the tunnel 28. In such case, routing table(s) of the IPsec gateway 12 must be adjusted accordingly. Further, to facilitate such packet transmission, the firewall of the L2TP network server 16 should allow for IPsec and IKE traffic from the IPsec gateway 12 and should also allow L2TP traffic between itself and the Public Internet 24 while disallowing other traffic.

[0016] FIGURE 2 shows a second embodiment of a network architecture 100 for transmitting IPsec packets in accordance with the invention. The architecture 100 shares elements in common with the architecture 10 of FIG. 1 and therefore, like reference numerals designate like elements. The architecture 100 of FIG. 100 differs from the architecture 10 of FIG, 1 in one major respect. In the network architecture 100 of FIG. 2, the L2TP network server 16 does not enjoy a dedicated connection to a particular IPsec gateway, such as via the tunnel 28 in the network architecture 10 of FIG. 1. Instead, with the network architecture 100 of FIG. 2, the L2TP network server 16 can access any IPsec client, such as IP sec gateway 12 of FIG. 2, visible on the public Internet 24. (In the network architecture 100 of FIG. 2 both the IPsec gateway 12 and the L2TP network server 16 enjoy a connection to the same router (i.e., router 25) so that the server can receive L2TP-wrapped IPsec packets from the IPsec gateway 12via the router 25 without actual connection to the public Internet 24.)

[0017] To facilitate IPsec packet transmission, the L2TP network server 16 of FIG. 2 must distribute publicly routable addresses to IPsec clients, such as IPsec gateway 12 of FIG. 2. Otherwise, the IPsec gateway 12 of FIG. 2 could not readily communicate with the L2TP network server 16. Also, the L2TP network server 16 must have sufficiently relaxed firewall rules to allow IPsec and IKE traffic from any IP address.

[0018] Having the L2TP network server 16 accessible through the public Internet 24 affords flexibility but incurs the potential for delay as packets are routed first through the public Internet 24 to the server (or in the case of FIG. 2, through the router 25 to the L2TP server) and then ultimately from the server to the destination. By comparison, the network architecture 10 of FIG. 1 avoids this potential difficulty since the L2TP network server 16 and IPsec gateway 12 both lie on the same local network.

[0019] FIGURE 3 illustrates a third network architecture 1000 for facilitating opportunist encryption between first and second IPsec clients 120 and 140, each typically comprised of an IP security device serving a corresponding one of computers 150_1 and 150_2, respectively. In the embodiment of FIG. 3, each of the IPsec clients 120 and 140 has a connection though a separate one of ISP networks 260_1 and 260_2 and NAT devices 250_1 and 250_2, respectively, to the public Internet 240.

[0020] To securely exchange IPsec packets, each of the IPsec clients 120 and 140 opens a separate one of L2TP tunnels 280_1 and 280_2, respectively, to a L2TP network server 160 configured in the same manner as the L2TP network server 16 of FIGS. 1 and 2. With the tunnels 280_1 and 280_2 opened to the IPsec clients 120 and 140, respectively, the L2TP network server 160 allows the two IPsec clients to establish a security association. After having established a security association with each other, each IPsec client can send an IPsec packet to the other via the L2TP network server 160. With tunnels 280_1 and 280_2 open to the IPsec clients 120 and 140, respectively, the L2TP network server 160 can communicate the L2TP-wrapped IPsec packet from one IPsec client to another while avoiding any transmission difficulties through each of the NAT devices 250_1 and 250_2.

[0021] The network architecture 1000 of FIG. 3 depicts a single L2TP network server 160 that serves both of the IPsec clients 120 and 140. Under such circumstances, the

L2TP network server would distribute to each IPsec client a private realm address identifying the server to allow each IPsec clients to communicate with the server in order for each IPsec client to open a corresponding one of the tunnels 280_1 and 280_2. In the event of multiple L2TP network servers, each would need to distribute a publicly routable address to the IP client served by each server.

[0022] Implementation of the IPsec packet transmission method of the invention places few requirements on the IPsec gateway 12 of FIGS. 1 and 2. Indeed, in the public implementation of FIG. 2 the IPsec gateway 12 need not even be aware that anything special is taking place. The only requirements are the usual ones for an IPsec gateway: that it be visible on the Public Internet 24, that it sees the L2TP network server 16 and that it knows the public part of the keys used by the IPsec clients, such as IPsec client 14 during authentication.

[0023] In the case where the L2TP network server 16 of FIGS 1 and 2 is distributing private-realm addresses to the IPsec clients, such as the IPsec client 14, the IPsec gateway must have routing table entries to appropriately route packets for these addresses through the L2TP network server.

[0024] The requirements for the L2TP network server 16 and 160 differ for different implementation scenarios. In all cases, the L2TP network server must be visible to the IPsec clients. In addition, the L2TP network server 16 should use the authentication mechanism in both L2TP and PPP and it should turn off packet compression. The security mechanisms of L2TP and PPP are rudimentary and insufficient to guard against denial of service attacks but they do make the hackers' job harder. Compression is useless here since the packets are encrypted before being relayed to PPP for compression. Depending on the scenario, the L2TP network server will distribute private-realm or public-realm addresses to the IPsec clients and thus must have a suitable range of addresses to distribute.

[0025] Since the L2TP network server introduces routing delays and potential denial of service attacks, it should only be used when a NAT device or incompatible firewall is interfering with the IPsec traffic. The IPsec client must therefore have access to a 'NAT discovery service' that will help it determine whether the L2TP tunnel is required. This service can take many forms but the simplest, a UDP service that echoes the source address and port it sees the request coming from, is sufficient. Placing this NAT discovery service on the same machine as the LNS seems simplest and most effective. In embodiment of FIG. 1 the LNS and the IPsec gateway are coupled together and thus it might prove useful to reflect this association by using related domain names like ipsec.corporate.domain.net and l2tp.corporate.domain.net. This would facilitate the IPsec client's job of locating a suitable L2TP server for a given IPsec gateway.

[0026] Implementation of the IPsec packet transmission method of the invention requires that each IPsec client support the L2TP network server in client mode and IPsec. In both cases, the client must of course be configured appropriately for the chosen scenario (public and private keys, knowledge of the IPsec gateway and LNS addresses, etc.). In addition, the network connection establishment must be modified to perform NAT discovery and, if appropriate, open the L2TP tunnel before establishing the IPsec security association.

[0027] The above-described embodiments merely illustrate the principles of the invention. Those skilled in the art may make various modifications and changes that will embody the principles of the invention and fall within the spirit and scope thereof.